

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

8/11/2009

SUBJECT:

Vulnerabilities in Microsoft Active Template Library Could Allow Remote Code Execution (MS09-037)

OVERVIEW:

Vulnerabilities have been discovered in Microsoft Active Template Library (ATL) that could allow an attacker to take complete control of an affected system. ATL is a set of pre-packaged programs that allow developers to create feature-rich applications. Exploitation may occur if a user visits a specifically crafted web page or opens a file which takes advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Microsoft Outlook Express 5.5 & 6
Windows Media Player 9, 10, & 11
Windows ATL Component
DHTML Editing Component ActiveX Control
Microsoft MSWebDVD ActiveX Control

RISK:

Government:

Large and medium government entities: High
Small government entities: High

Businesses:

Large and medium business entities: High
Small business entities: High

Home users: High

DESCRIPTION:

Multiple vulnerabilities associated with Microsoft's implementation of Active Template Library (ATL) have been discovered. ATL allows a developer

the ability to create custom objects to quickly interface with Component Object Model (COM) features, such as ActiveX controls. These vulnerabilities can be exploited when a user visits a specially crafted web page or opens a specially crafted file. This leads to memory corruption allowing the attacker to execute code in the context of the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

This advisory addresses issues in core Windows components and is needed to correct all issues caused by vulnerable ATL headers whereas Bulletin 2009-046, issued July 28, 2009, addressed the Internet Explorer components of this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Remind users not to open email attachments from unknown or un-trusted sources.

If you believe you have been affected by targeted attacks exploiting this vulnerability, please follow your organization's policies for incident reporting.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS09-037.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0020>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0901>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2494>

Security Focus:

<http://www.securityfocus.com/bid/35982>

<http://www.securityfocus.com/bid/35828>

<http://www.securityfocus.com/bid/35832>

<http://www.securityfocus.com/bid/35585>

<http://www.securityfocus.com/bid/35558>